# An Integrated Specification Framework for Embedded Systems

Marius C. Bujorianu[†],Manuela L. Bujorianu[*]
[†]University of Kent/Computing Laboratory, Canterbury, UK
[*]University of Twente/Faculty EWI, Enschede, The Netherlands

Abstract— In this paper, we address the complex issue of representation of continuous behaviour of the environment of the embedded controllers. In our approach, we propose two novel ideas. One is to consider the weak solutions to describe the evolution of the dynamical systems. The second novelty is to make available, at the design stage, the information about concurrent evolutions of the environment. We propose a new logic called the Hilbertian logic for representing continuous behaviours. Then, we use the causal order relations to integrate this logic with a probabilistic process algebra. For the resulting specification framework, we construct a denotational semantics rich in mathematical properties.

Keywords: embedded systems, causal order relations, weak solutions, probabilistic process algebra.

## I. Introduction

The spectacular recent developments in embedded systems raise new research issues. The embedded controllers become more sophisticated and they are now able to exploit complex information about their environment. Until now, the controllers were using sensor based measurements and therefore their possible actions were severely limited. The new challenges for embedded and ubiquitous computing need to consider, for example, the non-linear effects of global warming or the advanced implant technology that makes possible complex cardiac implants. In all these applications the environments have complex continuous behaviors permanently changing. Moreover, different continuous phenomena may occur simultaneously and then concurrency needs to be considered in the controller design process.

In order to support the design of a new generation of embedded controllers, it is necessary to develop a knowledge representation system that needs to meet the requirements identified above. In this paper, we introduce the fundamentals of a specification framework focused on:

1) the representation of mathematical properties of behaviors described by complex differential equations (possibly with partial derivatives);
2) knowledge representation should be made formally by defining, eventually, a suitable logic;
3) the ability to make available the information about concurrent evolution of the environment at the design stage.

These targets are very ambitious and their achievement involves a multi-staged investigation and international collaboration. In this paper, we present a preliminary investigation of the basic principles that should support such a framework.

The first challenge is addressed by implementing a common practice in continuous mathematics. When the solutions of differential equations can not be calculated or they are computationally unfeasible, the mathematicians can still obtain useful information by considering the so-called weak solutions (or solutions in the sense of distributions). We present an algebraic formalization of the weak solutions that does not involve the use of distributions. Therefore, this approach is very general and it can be applied to very complex physical or biological phenomena.

The second challenge is addressed by introducing a new logic, called Hilbertian logic, for representing the weak solutions. We interpret this logic in the class of semi-dynamical systems, a functional analysis based formalization of continuous phenomena. We use the name "Hilbertian" in honour of the mathematician and logician David Hilbert who pioneered the functional analysis methods and their applications in continuous mathematical modelling.

To the third challenge we devote most of our effort. We use the theory of causal orders from Petri nets to represent the simultaneous occurrences and the causal dependencies of continuous phenomena in a physical or biological environment. These phenomena are weak solutions associated to some differential operators and they are specified in the Hilbertian logic as we have discussed before. Moreover, the information about concurrency is made available at the design stage by integrating the Hilbertian logic with a probabilistic process algebra necessary to describe the behavior of the discrete controller. This process algebra has been already investigated in [17], [16], and it has a causal order denotational semantics.

The major advantage of this specification framework consists of a denotational semantics rich in mathematical properties. We illustrate its versatility by specifying density properties, which are discrete approximations of continuous changes in the environment behavior. This semantic framework constitutes a robust basis for future developments.

## II. Motivation for Hilbertian Formal Methods

The explosive growth in microelectronics, biomedical implants, and ubiquitous computing raises challenges to formal methods that would have been hard

to consider seriously a decade ago. Microprocessors, sensor networks and various controllers function now in the most unexpected physical environments. In medicine, there are electronic implants in the most sensitive parts of the human body like heart and brain. The bottom of the sea and the remote windmills are monitored by sensor networks exhibiting complex behaviors like adaptivity, self-management, etc. This list of examples can become even longer considering wireless communications, robotics and the classical applications of hybrid systems (chemical industry, automotive systems, power and nuclear plants). A major characteristic of these systems is that they operate in a physical continuous environment, and the interaction with this environment can be complex. Traditionally, this class of applications has been associated with embedded systems. The research in embedded systems has focused mainly on real time constraints and resource limitations. The continuous dynamics of the environment has very peculiar features like nonlinearity, uncertainty, etc. Usually, these have been abstracted away by drastic discretizations: the environment evolution is measured using a finite set of sensors. The real values of these parameters were the only continuous aspects considered in the design of an embedded controller. In control engineering and hybrid systems, there are cases when the continuous aspects are fully considered in the form of continuous dynamical systems. However, there are subtleties regarding their practical use: these dynamical systems are, in general, designed by humans (engines, cars, planes, trains, etc). These systems are simpler and less uncertain than the physical processes from nature and biological systems. When continuous processes are considered in their full generality there is little or no use at all of formal methods (like in gene regulatory networks, control engineering, bioengineering, etc). In this paper, we address the issue of constructing a semantic framework that bridges the formal methods and the continuous physical models. The intelligent embedded systems need to meet the requirements of modern control (prevision, adaptivity, learning, self-management) and critical safety requirements. To achieve that, they will consider sophisticated environment representations. The main obstacles in using physical features in formal methods are due to the different nature of the semantics. The difference between the semantics of the discrete controller and the continuous environment is, in fact, very deep and it acts in multiple dimensions. The most obvious difference is the density of trajectories of the environment behavior.

## III. Mathematical Preliminaries

In this section we provide background material on concurrency modelled as a poset (an approach originating from Petri nets [2]) and on semidynamical systems.

### A. Concurrency relations and causal posets

A complete lattice is a partially ordered set, in which every subset has a least upper bound and a greatest lower bound. A conditionally complete lattice is a lattice which has the property that every non-void bounded subset has a least upper bound and a greatest lower bound.

We consider a set $B$ and the following relations [2]:
• the concurrency relation: $co \subset B \times B$ is a symmetric nonreflexive relation ($co \cap id_B = \emptyset$);
• the causal relation: $li \subset B \times B$ is a nonreflexive relation, i.e. $li \cap id_B = \emptyset$;
such that the following interrelating properties hold:

$$co \cap li = \emptyset$$

and

$$co \cup li = B \times B - id_B.$$

The following properties hold:
i) $li = li^{-1}$;
ii) $li = B \times B - co$.
A partial order $\prec \subseteq B \times B$ is called a causal order iff

$$\prec \cup \succ = li.$$

Let $\prec$ be a causal order. We consider the following concepts [2]:
• $\preccurlyeq = \prec \cup id_{|B}$;
• $\succ = \prec^{-1}$;
• $li =: \prec \cup \succ \cup id_{|B}$;
• $l \subseteq B$ is a li-set iff $(\forall a, b \in l) : (a, b) \in li$ or $(b, a) \in li$;
• $l \subseteq B$ is a line iff $l$ is a li-set maximal w.r.t. $li$: $(\forall a \in B - l), (\exists b \in l) : (a, b) \in (B \times B) - li$;
• $c \subseteq B$ is a co-set iff $(\forall a, b \in co) : (a, b) \in co$ or $(b, a) \in co$;
• $c \subseteq B$ is a cut iff $c$ is a co-set maximal w.r.t. co: $(\forall a \in B - c), (\exists b \in l) : (a, b) \in (B \times B) - co$.

### B. Dynamical systems

Semi-dynamical systems [21] might be thought of as restrictions of dynamical systems to the positive time interval. They represent solutions of partial differential equations (possibly in the sense of distributions) and they are not necessary continuous.

Let $X$ be a Polish space (i.e. a topological space homeomorphic with the image of a complete separable metric space). We consider $X$ equipped with its Borel $\sigma$-algebra $\mathcal{B}$ (i.e. the $\sigma$-algebra generated by all open sets). We adjoin an extra point $\Delta$ (the cemetery or deadlock point) to $X$ as an isolated point,

$$X_\Delta = X \cup \{\Delta\}.$$

Let $\mathcal{B}(X_\Delta)$ be the Borel $\sigma$-algebra of $X_\Delta$.
The set of all bounded measurable numerical functions on $X$ denoted by $\mathbf{B}(X)$.

Mathematically, this set can be thought of as a lattice (with the natural pointwise order between numerical functions), or as an additive monoid $(\mathbf{B}(X), +, 0)$.

These functions can be thought as abstract states (configurations) of the given system or, some formulas in an appropriate logic. Moreover, $\mathbf{B}(X)$ is also a Banach space with respect to the sup-norm and the natural pointwise algebraic operations which give its linear structure.

Definition 1: [15] A semi-dynamical system is a pair

$$(X, \phi)$$

where $\phi$ is a function

$$\phi : \mathbb{R}_+ \times X_\Delta \to X_\Delta$$

such that

1. $\phi$ is a measurable map;
2. $\phi(o, x) = x$;
3. $\phi(t_1 + t_2, x) = \phi(t_1, \phi(t_2, x))$;
4. $\phi(t, x) = \Delta \Rightarrow \phi(s, x) = \Delta, \forall s \geq t$;
5. $\phi(t, x) = \phi(t, y), \forall t > 0 \Rightarrow x = y$.

The semi-dynamical system $\phi$ is called transient if there exists $(A_n) \subset \mathcal{B}$ such that $X = \bigcup_{n\in\mathbb{N}} A_n$ and

$$m\{t \in [0, \infty) | \phi(t, x) \in A_n\} < \infty, \ \forall x \in X$$

where $m$ is an appropriate measure on $(X, \mathcal{B})$.
The kernel operator $V : \mathbf{B}(X) \to \mathbf{B}(X)$ is defined by

$$Vf(\cdot) = \int_0^\infty f(\phi(t, \cdot))dt \tag{1}$$

## IV. Behavioral specification

In modern control engineering (see, for example, the EU Hybridge project web site [11] for extensive references), the problems are formulated in a global manner. For example, quite often engineers and applied mathematicians use measurable sets of system trajectories (often of continuum power). The trajectories themselves are dense and thus it is impossible to use specifications involving concepts like 'next state' and 'after $k$ steps the system...'. The trajectories form very rich algebraic and functional structures. System properties are often defined in terms of possible trajectories using advanced concepts of topology, functional analysis and probability theory. In contrast, probabilistic methods in computer science are based on explicit state changes, where the concept of next state is fundamental. These methods, from an engineering (whether this is financial, medical or safety critical systems) point of view, could be characterized as been local (the vicinity given by the possible next states) or observational (the system behavior is given by observing the state changes). Probabilistic specification and verification (using model checking) are now mature and rapidly growing. A severe limitation of these methods is that they are strictly local (which means a clear underlying transitional structure).

In this section, we propose a logic for specifying properties of behavioral models called Hilbertian Logic (HiL). This logic can be used in conjunction with the specification language Z [22] for a complete mathematical language. Z offers a mathematical notation familiar to the mathematicians, including differentiation and integration [12].

### A. The Hilbertian Logic

The syntax

Consider a generic collection of types, called Hilbertian types. Each type models a (partial) differential operator corresponding to the equations that govern the dynamics of the environment.

The terms of a given type $T$ are generated by the following grammar

$$f := \mathbf{1} | \perp | \top | \wp.f | f \odot f | f : f | f \stackrel{\circ}{-} c | \inf(f, f) | \sup(f, f)$$

To each type $T$ we attach two supertyped $\wp_T$ and $E_T$ and the terms of type $\wp_T$ are of the form $\wp.f$ with $f$ ranging the terms of type $T$. The terms of type $E_T$ are of the form $\sup_{n\in\mathbb{N}} p_n$ with $p$ ranging the terms of type $\wp_T$. Denote by $\mathcal{F}$ the set of terms.

The formulas are defined as equalities or inequalities between terms. The (in)equalities, where the left hand side term is of type $E_T$, are called trace formulas.

Interpretation as deterministic dynamical systems

Let $(X, \phi)$ be a transient semi-dynamical system. The interpretation of a term $f \in \mathcal{F}$ is a function $f : X \to \mathbb{R}$ which belongs to $\mathbf{B}(X)$. Then

$\mathbf{1}(x) := 1, \forall x \in X$
$\perp (x) := 0$
$\top(x) := M$, where $M$ is a constant large enough
$(f \odot g)(x) := f(x) + g(x)$

$$(f : g)(x) := \begin{cases} f(x) - g(x) & , \text{ if } f(x) \geq g(x) \\ 0 & , \text{ otherwise} \end{cases}$$

$$(f \stackrel{\circ}{-} c)(x) = \begin{cases} f(x) - c & , \text{ if } f(x) \geq c, \forall x \in X \\ 0 & , \text{ otherwise} \end{cases}$$

The infimum and supremum are defined pointwise. The action of $\wp$ to a formula $f$ is given by

$$(\wp.f)(\cdot) = Vf(\cdot)$$

The global properties of weak solutions of partial differential equations can be traced back to the Poincare's sweeping method. In each system state $x$, a weak solution is characterized by a potential given by $Vf(x)$ in our approach.

The elements of $\mathbf{B}(X)$ can be thought of as terms in a Hilbertian logic associated to $(X, \phi)$.

Example 1: The following Hil specification

$$\begin{aligned} \frac{\partial V}{\partial t} &= 5(V : \frac{V^3}{3} : W) \\ \frac{\partial W}{\partial t} &= \frac{1}{5}(V : 0.8W \odot 0.7) \end{aligned}$$

defines the FitzHugh-Nagumo model [18]

$$\begin{aligned} \frac{\partial V}{\partial t} &= \frac{1}{\epsilon}(V - \frac{V^3}{3} - W) \\ \frac{\partial W}{\partial t} &= \epsilon(V - \gamma W + \beta) \end{aligned}$$

with $\gamma = 0.8$, $\beta = 0.7$, $\epsilon = 0.2$, where $V$ and $W$ are the membrane electrical potential, respectively the

cell's refractory potential.

An algebraic semantics

A basic space is defined as being a structure $< \mathbb{S}, \leq, \perp, \top, \odot >$ where:

($S_1$) $< \mathbb{S}, \leq, \perp, \top >$ is a lattice for which:

- $\perp$ the minimal element and $\top$ the greatest element;
- the lattice $(\mathbb{S}\backslash\{\top\}, \leq_{|\mathbb{S}\backslash\{\top\}}, \perp)$ is lower complete and upper conditionally complete;
- $\leq$ is called the essential order; we denote by $\vee$ resp. $\wedge$ the supremum resp. infimum w.r.t. $\leq$;
- $\perp$ is called the nil action; $\top$ is called deadlock;

($S_2$) $(\mathbb{S}, \odot, \perp)$ is a monoid for which:

- $s = \perp$ if $s \odot s = \perp$ $(\forall s \in \mathbb{S})$;
- $s \odot \top = \top$ $(\forall s \in \mathbb{S})$;

($S_3$) the following compatibility axioms hold:

- $s \odot (a \vee b) = (s \odot a) \vee (s \odot b)$ $(\forall a, b, s \in \mathbb{S})$;
- $a \odot b = (a \wedge b) \odot (a \vee b)$ $(\forall a, b \in \mathbb{S})$.

The residual of $a$ by $b$, denoted by $a : b$, is the greatest element (if exists) such that

$$b \odot (a : b) \leq a.$$

The semantics of a type $T$ of HiL is a basic space denoted by $\mathbb{S}_T$. The semantics of a term of type $T$ is an element of $\mathbb{S}_T$.

The operators $\odot$ and : denote addition, respectively substraction. The logical operators $\inf, \sup, \perp, \top$ are interpreted by their obvious correspondent in a basic space.

The semantics of the logical constant 1 is the neutral of the basic space monoid.

Two elements $a, b \in \mathbb{S}$ are called strongly dual, denoted by $a \perp b$, if $a \wedge b = \perp$. We denote the class of orthogonal elements of $a$, by $a^{\perp}$, i.e.

$$a^{\perp} =: \{s \in \mathbb{S}; a \perp s\}.$$

Let $\mathbb{S}$ be a basic space. The specific order $\leq_{\odot}$ on $\mathbb{S}$ is defined by

$$a \ \leq_{\odot} b \overset{def}{\Leftrightarrow} (\exists c \in \mathbb{S}) : b = a \odot c.$$

We denote by $\bigvee_{\odot}$ resp. $\bigwedge_{\odot}$ the supremum resp. infimum in this order (if they exist).

A basic space $\mathbb{S}$ has the decomposition property if for any $s, s_1, s_2 \in \mathbb{S}$ such that $s \leq s_1 \odot s_2$ there exists $t_1, t_2 \in \mathbb{S}$ such that $t_1 \leq s_1,\ t_2 \leq s_2,\ s = t_1 \odot t_2$.

Proposition 1: Every basic space has the decomposition property.

Proof: Consider $t_1 =: s \wedge s_1$ and $t_2 =: s : t_1$. Then $t_1 \leq s_1$ and $t_2 = (s : s_1) \vee \perp$ so $t_2 \leq s_2$.□

Lemma 2: Let $\mathbb{S}$ be an basic space and $s, a, b \in \mathbb{S}$. Then

i) $a \odot b \geq a \vee b$

ii) if $a \leq b$ then $s \odot a \leq s \odot b$

iii) $(a \bigwedge_{\odot} b) \odot (a \bigvee_{\odot} b) = a \odot b$

iv) if $a, b \leq s$ and $a \perp b$ then $a \odot b \leq s$

Proof:

i) $a \odot b = (a \wedge b) \odot (a \vee b) \geq a \vee b$

ii) $(\ s \odot a) \wedge (s \odot b) = s \odot (a \wedge b) = s \odot a$

iii) Suppose that every pair $a, b \in \mathbb{S}$ has a supremum $a \bigvee_{\odot} b$. Since $a \odot b \geq_{\odot} a$ and $a \odot b \geq_{\odot} b$ it follows that $a \odot b \geq_{\odot} a \bigvee_{\odot} b$. Define $c = (a \odot b) : (a \bigvee_{\odot} b)$. Then
$c \odot (a \bigvee_{\odot} b) = a \odot b \leq_{\odot} (a \bigvee_{\odot} b) \odot b$
so $c \leq_{\odot} b$ and similarly $c \leq_{\odot} a$. On the other hand, if $c' \leq_{\odot} a$ and $c' \leq_{\odot} b$, then
$c' \odot (a \bigvee_{\odot} b) = (c' \odot a) \bigvee_{\odot} (c' \odot b) \leq_{\odot} a \odot b$
so $c' \leq_{\odot} c$, and it follows that
$c = (a \bigwedge_{\odot} b) \Leftrightarrow (a \bigwedge_{\odot} b) \odot (a \bigvee_{\odot} b) = a \odot b$;

iv) $a \odot b = (a \wedge b) \odot (a \vee b) = a \vee b$ and
$(a \odot b) \wedge s = (a \vee b) \wedge s = (a \wedge s) \vee (b \wedge s) = a \vee b = a \odot b$.□

Proposition 3: The specific order is coarser than the essential order, i.e.

$$\leq_{\odot} \subseteq \leq$$

Proof: $a \ \leq_{\odot} b \Leftrightarrow \exists c \in \mathbb{S}$: $b = a \odot c \geq a \vee c \Rightarrow a \leq b$.□

Proposition 4: Any basic space is a distributive lattice.

Proof: It is enough to show that $a \wedge s = b \wedge s$ and $a \vee s = b \vee s$ imply $a = b$. But
$a \odot s = (a \wedge s) \odot (a \vee s) = (b \wedge s) \odot (b \vee s) = b \odot s \Leftrightarrow a = b$.
□

A subset $A$ of a basic space is called linearisable if

(L) $s \odot a \leq s \odot b$ implies $a \leq b$ $(\forall a, b \in A)$.

We define the order topology $\tau_{\leq}$ on $< \mathbb{S}, \leq >$ as follows. A net $(a_i)_{i \in I}$ converges to $a$, $(a_i)_{i \in I} \underset{\tau_{\leq}}{\rightarrow} a$, iff ( $(a_i)_{i \in I}$ is increasing and dominated and $\bigvee\limits_{i \in I} a_i = a$ ) or ( $(a_i)_{i \in I}$ is decreasing and $\bigwedge\limits_{i \in I} a_i = a$ ).

Analogously, one can be defined the specific order topology $\tau_{\leq_{\odot}}$ on $< \mathbb{S}, \leq_{\odot} >$.

Proposition 5: The superposition is continuous in the order topology.

Proof: We prove that the following relations hold in any basic space:

($\mathrm{ID}_{\mathbf{1}}$) for any increasing and dominated net $(s_i)_{i \in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigvee_{i \in I} (s \odot s_i) = s \odot (\bigvee_{i \in I} s_i) \tag{2}$$

($\mathrm{ID}_{\mathbf{2}}$) for any net $(s_i)_{i \in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigwedge_{i \in I} (s \odot s_i) = s \odot (\bigwedge_{i \in I} s_i) \tag{3}$$

We prove first ($\mathrm{ID}_{\mathbf{2}}$). We set $a =: \bigwedge_{i \in I} s_i$ and $b =: \bigwedge_{i \in I} (s \odot s_i)$. Observe that $s \odot a \leq b$. From $b \leq s \odot s_i$ we obtain $b : s \leq s_i$ $(\forall i \in I)$. Therefore
$b : s \leq a \Leftrightarrow b \leq s \odot a \Leftrightarrow \bigwedge_{i \in I} (s \odot s_i) = s \odot (\bigwedge_{i \in I} s_i)$.
We prove now ($\mathrm{ID}_{\mathbf{1}}$). We set $a =: \bigvee_{i \in I} s_i$ and $b =: \bigvee_{i \in I} (s \odot s_i)$. Observe that $s \odot a \geq b$. From $b \geq s \odot s_i$ we obtain $b : s \geq s_i$ $(\forall i \in I)$. Therefore
$b : s \geq a \Leftrightarrow b \geq s \odot a \Leftrightarrow \bigvee_{i \in I} (s \odot s_i) = s \odot (\bigvee_{i \in I} s_i)$.□

Remark 1: The latticeal operations $\vee$ and $\wedge$ are continuous in the order topology.

Lemma 6: The following relations hold in any basic space:

($\mathbf{GD_1}$) for any increasing and dominated net $(s_i)_{i\in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigvee_{i\in I}(s \bigwedge s_i) = s \bigwedge(\bigvee_{i\in I} s_i);$$

($\mathbf{GD_2}$) for any net $(s_i)_{i\in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigwedge_{i\in I}(s \bigvee s_i) = s \bigvee(\bigwedge_{i\in I} s_i).$$

Proof: We prove first ($\mathbf{GD_2}$). We define $a =: \bigwedge_{i\in I} s_i$ and $a_i =: s_i : a$, $(\forall i \in I)$. We have $\bigwedge_{i\in I} a_i =\perp$ . We have $s \wedge a \leq (s \odot a_i) \vee (a \odot a_i) = (s \vee a) \odot a_i$. Thus $\bigwedge_{i\in I}(s \vee s_i) \leq \bigwedge_{i\in I}((s \vee a) \odot a_i) = s \vee a$. The converse inequality is immediate.
We prove now ($\mathbf{GD_1}$). We consider $a =: \bigvee_{i\in I} s_i$ and $a_i =: a : s_i$, $(\forall i \in I)$. Obviously $\bigwedge_{i\in I} a_i =\perp$ . We have $s \vee s_i \leq (s \odot a_i) \wedge (s_i \odot a_i) = (s \wedge s_i) \odot a_i \leq \bigvee_{i\in I}((s \wedge s_i) \odot a_i)$. Thus $s \wedge a \leq \bigvee_{i\in I}(s \wedge s_i)$. □

B. Probabilistic process algebra PPA

The embedded controllers are usually networked (i.e. concurrent) and they behave probabilistically. Then their behavior can be better described using a probabilistic process algebra. We choose PPA [16] , a probabilistic extension of a kernel of the Lotos language admitting a true concurrency semantics. The denotational semantics, based on causal ordering, makes easier the integration. PPA has also an operational semantics useful for design and implementation.

1) The syntax
: Let $Act$ be a finite alphabet and $\mathcal{L}$ be the set of formulas generated by the following grammar:

$$F ::= 0 \mid \surd \mid a; F \mid F + F \mid F +_p F \mid F||_G F \mid F \gg F \mid F[> F.$$

The operators $+_p$ and $+$ bind equally strong and $p \in (0, 1)$.

The constants 0 and $\surd$ denote inaction, respectively successful termination. $a; F$ is the action prefix. The operators $+, ||_G, \gg, [>$ denote, respectively, the choice, parallel composition, enabling and disruption. The operator $+_p$ is the probabilistic choice: $F +_p G$ means that $F$ or $G$ are executed nondeterministically, $F$ with the probability $p$ and $G$ with the probability $1 - p$.

The $PPA$ consists of those formulae that satisfy the $ppa$ predicate

$$PPA \triangleq \{F \in \mathcal{L} \mid ppa(F)\}$$

where $ppa : \mathcal{L} \to Bool$ is defined as:

$ppa(0) \triangleq true$, $ppa(\surd) \triangleq true$
$ppa(F_1[> F_2) \triangleq \neg pc(F_1) \wedge \neg pc(F_2) \wedge ppa(F_1) \wedge ppa(F_2)$
$ppa((F_1 + F_2) \triangleq \neg pc(F_1) \wedge \neg pc(F_2) \wedge ppa(F_1) \wedge ppa(F_2)$
$ppa(op\ F) \triangleq ppa(F)$ for $op \in \{a; , \backslash, []\}$
$ppa((F_1\ op\ F_2) \triangleq ppa(F_1) \wedge ppa(F_2)$ for $op \in \{||_G, \gg\}$
$ppa(F_1 +_p F_2) \triangleq ppc(F_1 +_p F_2) \wedge ppa(F_1) \wedge ppa(F_2)$

The predicate $ppc : \mathcal{L} \to Bool$ is defined by

$ppc(B_1 +_p B_2) \triangleq (ppc(B_1) \vee B_1 = \tau; B_1^{'}) \wedge (ppc(B_2) \vee B_2 = \tau; B_2^{'})$
$ppc(B_1 \gg B_2) \triangleq ppc(B_1)$,
$ppc(op\ B) \triangleq ppc(B)$ for $op \in \{\backslash, []\}$
and $ppc$ is false for all other formulae.

The predicate $pc(B)$ denotes the fact that the formula $B$ has a probabilistic choice at the component level. The function $pc : \mathcal{L} \to Bool$ is defined as follows:

$pc(B_1 +_p B_2) \triangleq true$
$pc(B_1 \gg B_2) \triangleq pc(B_1)$
$pc(B_1||_G B_2) \triangleq pc(B_1) \vee pc(B_2)$
$pc(op\ B) \triangleq pc(B)$ for $op \in \{\backslash, []\}$.
and $pc$ is false for all other syntactical constructs.

2) The causal order semantics
: The poset semantics of Lotos has been fully explored in [16], where a new type of causal orders, called bundle event structures, has been introduced precisely to give semantics for process algebra.

A bundle event structure $\mathcal{E}$ [16] is a quadruple $(E, \#, \mapsto, l)$ with:
(i) a set of events $E$;
(ii) the conflict relation

$$\# \subseteq E \times E$$

which is irreflexive and symmetric;
(iii) the bundle relation

$$\mapsto \subseteq \mathcal{P}(E) \times E;$$

(iv) the action-labelling function

$$l : E \to Act,$$

such that $\forall X \subseteq E$, $e \in E$:

$$X \mapsto e \Rightarrow (\forall e', e'' \in X : e' \neq e'' \Rightarrow e' \# e'').$$

The semantics of PPA is then given in a probabilistic event structure.
A probabilistic event structure [17] is a tuple $(\mathbb{E}, d)$ consisting of
- an extended bundle event structure $\mathbb{E} = (E, \rightsquigarrow, \mapsto, l)$
- a probability function

$$d : E \nrightarrow (0, 1),$$

such that

$$\begin{aligned} \forall e \ &\in\ dom(d) : \exists Q \subseteq dom(d) : \\ (e \ &\in\ Q) \wedge (Q \text{ is a cluster}) \wedge \\ (\sum_{e'\in Q} d(e') \ &=\ 1. \end{aligned}$$

## V. Integrated specification of embedded processes

Embedded systems work in a real life environment, whose behaviour is highly unpredictable. In many situations, these behaviours are governed by (partial) differential equations that can be changed by discrete events (triggers). These behaviours are difficult to be studied by classical mathematical tools. Solutions of partial equations are partial system evolutions, thus we can not derive conclusions on the global evolutions.

The mechanism used to integrate the specification notations is essentially observational. It consists of the recording that an external observer observes the evolutions of the physical environment, as well as the changes in these evolutions determined by the controller actions. This observation process can be interpreted in an abstract computational way (as in the case of event structures, for example) or strictly in a physical way like in biomedical applications. For example, consider the case of a cardiac stimulator: the real observer is the cardiac specialist that effectively records a sequence of heart activity potentials. These potentials can be easily specified in HiL and they compose sequentially. When a dangerous potential appears, the stimulator activates electrical impulses that trigger the firing of excitatory heart potentials. This sequential evolution is modelled using a $li$ relation. The change of potential is done in a smooth continuous way. This continuous change can be modelled either by functional composition (i.e. we consider a globally defined function) or by properties imposed on the $li$ relation. With this respect, the poset approach is very expressive. Continuous changes are modelled by the density property. Moreover, one can distinguish degrees of density. Another example is that of a monitor of patients with brain affections. The brain activity is monitored as the sequence of electrical brain potentials (the encephalogram). When dangerous potentials are uncounted, the monitor can alert immediately the medical staff or even can take some emergency actions (like dropping a medicine in a perfusion). Obviously, there are cases when the physical process is simultaneously observed by different devices. This concurrent evolution is modelled by the $co$ relation. The $li$ and $co$ relations can be pasted into a single order relation called causal order. In a computationally abstract sense, this order might be use to give semantics to different kinds of concurrent systems specified for example using process algebra or Petri nets. Further advantages for using posets come from their recent use in formal verification.

### A. Embedded processes

The basic ingredients of our framework are

- the causality relation, modelled by some partial order relations ($a \prec b$ means the event $a$ is the cause of $b$), and
- an algebraic structure (called here embedded processes).

Two system evolutions $a, b$ that are causal independent (i.e. $a \not\prec b$ nor $b \not\prec a$) can take place simultaneously (true concurrency).

We define event spaces that represent the mathematical model of dynamics of the environment recorded by an embedded system.
The elements of an event space are then decorated with elements of a basic space, a mathematical frame, in which many biological potentials and dynamical systems can be defined.

An event space is a structure

$$< \mathbb{M}, \prec, \#, \mapsto, Act \cup \{*\}, \complement >$$

such that
($M_0$) $< \mathbb{E}, \#, \mapsto, Act \cup \{*\}, \complement >$ is a bundle event structure, where $\mathbb{E} = \{(\alpha, \beta) \in \lessdot\}$, such that if $\alpha = (a, b)$ and $\beta = (b, c)$, then $\alpha \mapsto \beta$.
($M_1$) $< \mathbb{M}, \prec >$ is a lower complete semi-lattice. The order $\prec$ is called the causal order. We denote by $\curlywedge$ (resp. $\curlyvee$) the infimum (resp. supremum if exists) of this semi-lattice.
($M_2$) If $(\alpha_i)_{i \in I}$ is increasing net dominated in $\mathbb{M}$ by $\alpha$, $\alpha \in \mathbb{M}$, then there exists $\underset{i \in I}{\curlyvee} \alpha_i$.
The symbol $*$ denotes the environment transitions and the elements of $Act$ denote the controller transitions.

A probabilistic event space is an event space

$$< \mathbb{M}, \prec, \#, \mapsto, Act \cup \{*\}, \complement, d >$$

such that $< \mathbb{E}, \#, \mapsto, Act \cup \{*\}, \complement, d >$ is a probabilistic event structure and the probability function $d$ is not defined exactly for those events labelled with the $*$ symbol.

We have now the all necessary ingredients to define the major concept of this paper.

An embedded process is a tuple

$$< \mathbb{M}, \mathbb{S}, \ell, Act, \complement >,$$

where
- $< \mathbb{M}, \prec, \#, \mapsto, Act, \complement >$ is an event space,
- $< \mathbb{S}, \leq, \bot, \top, \odot >$ is a basic space, and
- $\ell$: $\mathbb{M} \to \mathbb{S}$ is an injective isotone labelling function such that, if $\mathbb{B} = \ell(\mathbb{M})$ then:

($P_1$) $\ell(\alpha \curlyvee \beta) \geq_{\odot} \ell(\alpha) \vee \ell(\beta)$ if $\alpha \curlyvee \beta$ exists
($P_2$) if $\ell(\alpha \curlyvee \beta) = \intercal$ and $\gamma \succ \alpha \curlyvee \beta$ then $\ell(\gamma) = \top$
($P_3$) $\bot \in \mathbb{B}$
($P_4$) $< \mathbb{B}, \leq_{|\mathbb{B}}, \wedge >$ is a lower complete semi-lattice of $< \mathbb{S}, \leq >$
($P_5$) $\mathbb{B}$ is linearisable;
($P_6$) $(\mathbb{B}, \odot, \bot)$ is a monoid;
($P_7$) The superposition is a continuous operation w.r.t the order topology on $\mathbb{B}$;
($P_8$) $\mathbb{B}$ has the decomposition property.

The elements of an embedded process are called basic occurrences and will be denoted by Greek letters: $\alpha$, $\beta$, etc. Their labels $\ell(\alpha), \ell(\beta)$ are called atomic processes. In the rest of this paper we identify these concepts.

In an embedded process, an event $\alpha$ is labelled with $\ell(\alpha)$, the denotation of a Hil term of the form $\wp.a$. This means that every event is an evolution of a semi-dynamical system $(X, \phi)$, which is equal with the function $a$ on the border.
The causal order $\preccurlyeq$ describes how these evolutions change over time. This could also mean a controller specification, or could be used to design a controller.

In the following we present three examples, illustrating the generality of the embedded process concept (and therefore the wise domain of possible applications).

Example 2: Let $\tau$ be Lebesgue measure on $\mathbb{R}^n$, let $X$ be an open set of $\mathbb{R}^n$ and let $a_{i,j}$ $(i, j = 1..n)$ be $\tau$-measurable functions satisfying the following conditions

- $a_{i,j} = a_{j,i}$
- there exists a real number $m \geq 1$ such that

$$\begin{array}{rcl} \frac{1}{m}\sum_{i=1}^{n}\xi_i^2 & \leq & \sum_{i,j=1}^{n} a_{i,j}(x)\xi_i\xi_j \leq m\sum_{i=1}^{n}\xi_i^2\,, \quad (4) \\ \forall x & \in & X, \forall(\xi_i)_{1\leq i\leq n} \in \mathbb{R}^n \end{array}$$

For any open set $V \subset X$ we denote by $\mathcal{H}(V)$ the set of real, continuous functions $h$ on $V$ such that the derivatives of first order of $h$ in the sense of distribution theory belong to $L^2_{loc}(\tau)$ and such that for any real function $f$ of class $C^\infty(V)$ with compact carrier, we have

$$\int_U \sum_{i,j=1}^{n} a_{i,j}\frac{\partial h}{\partial x_i}\frac{\partial f}{\partial x_j}d\tau = 0.$$

An embedded process consists on all positive functions $p$ for which $p_{|V} \in \mathcal{H}(V)$ for all open sets $V \subseteq X$.

Example 3: Let $D \subset \mathbb{R}^n$ be an open set and define the basic space $\mathcal{U}$ as a harmonic sheaf on $X$ such that:

- any $\mathcal{U}$-functions is of class $C^2$;
- $\mathcal{U}$ is non-degenerate at every point of $D$;
- the set of $\mathcal{U}$-regular sets is a base of $D$;

Then there exists a system of real functions $u_{i,j}, v_i, w$ $(i, j = 1..n)$ on $\mathbb{D}$ such that:

i) $u_{i,j} = u_{j,i}$;

ii) $(u_{i,j})$ is a non-zero positive definite matrix at any point of $D$;

iii) for any $\mathcal{H}$-function $h$, we have

$$\sum_{i,j=1}^{n} u_{i,j}\frac{\partial^2 h}{\partial x_i \partial x_j} + \sum_{i=1}^{n} v_i\frac{\partial h}{\partial x_i} + wh = 0;$$

iv) there exists an open, dense set $V \subset X$, such that $u_{i,j}, v_i, c$ are continuous on $V$, and such that any solution of the above equation on any open subset of $V$, is an $\mathcal{U}$-function.;

An embedded process consists on all positive functions $p$ for which $p_{|V} \in \mathcal{H}(V)$ for all open sets $V \subseteq X$.

Example 4: Let $D \subseteq \mathbb{R}^n$ be an open set, let the basic space $\mathbb{S}$ be the positive continuous real function on $D$, $a \in [\mathbb{S}]$ and let $(A_i)_{1\leq i\leq j}$, $B$ be first order differential operators of class $\mathcal{C}^\infty(D)$. For any open set $V \subseteq D$, let $\mathcal{H}(V)$ be the set of real functions $h \in \mathcal{C}^\infty(V)$ and satisfying

$$\sum_{i=1}^{j}(A_i)^2 h + Bh + ah = 0.$$

Suppose that the Lie algebra generated by the operators $A_i$ and $B$ for the operation

$$(\sum_{i=1}^{n} a_i\frac{\partial}{\partial x_i})\cdot(\sum_{i=1}^{n} b_i\frac{\partial}{\partial x_i}) = \sum_{i=1}^{n}(\sum_{j=1}^{n} a_j\frac{\partial b_i}{\partial x_j} - b_j\frac{\partial a_i}{\partial x_j})\frac{\partial}{\partial x_i}$$

is of rank $n$ at any point of $D$. An embedded process consists on all positive functions $p$ for which $p_{|U} \in \mathcal{H}(U)$ for all open sets $U \subseteq X$.

B. Specification of embedded system properties

In this subsection, we show the versatility of the integrated language to specify desirable properties of embedded systems. These properties include density and observability. Density is an intermediate property between discreteness and continuity. This property is very important in describing the environment behavior as a series of physical phenomena. The discrete controller is not always able to record a continuous succession of events and thus discreteness provides various ways of approximation. The corner stone to specify such properties consists in using partial order relations. The algebraic structure of an embedded process is rich enough to construct a theory of observability.

B1. Density property specification

An embedded process is called

- dense iff $\prec = \varnothing \Longleftrightarrow \forall\alpha, \beta \in \mathbb{B} : \alpha \prec \beta \Rightarrow \exists\gamma \in \mathbb{B} : \alpha \prec \gamma \prec \beta$;
- combinatorial iff $\preccurlyeq = (\prec)^+$;
- K-dense iff $(\forall l \in L)\ (\forall c \in C)\ l \cap c \neq \emptyset$;
- N-dense iff $(\forall\alpha, \beta, \gamma, \delta \in \mathbb{B})$ : $(\gamma\ co\ \beta\ \&\ \beta\ co\ \alpha\ \&\ \alpha\ co\ \delta\ \&\ \alpha\ li\ \gamma\ \&\ \gamma\ li\ \delta\ \&\ \delta\ li\ \beta) \Rightarrow (\exists e \in \mathbb{B} : e\ co\ \alpha\ \&\ e\ co\ \beta\ \&\ e\ li\ \gamma\ \&\ e\ li\ \delta)$;
- with finite intervals iff $(\forall\alpha, \beta \in \mathbb{B}) : |[\alpha, \beta]| < \infty$;
- boundedly discrete iff $(\forall\alpha, \beta \in \mathbb{B})\ (\exists n \in \omega)\ (\forall l \in L) : |[\alpha, \beta] \cap l| < n$.

An embedded process $\mathbb{B}$ is called continuous if for any Dedekind-cut [2] $(\mathbb{A}, \overline{\mathbb{A}})$ of $\mathbb{B}$ and any line $l$

$$|M(\mathbb{A}) \cap l| = 1.$$

If the embedded process $\mathbb{B}$ is continuous then $\mathbb{B}$ is dense [2].

Let $\mathbb{D} \subseteq \mathbb{M}$. We call $\mathbb{D}$

- dense in order from below (in $\mathbb{M}$) if for any $\alpha \in \mathbb{M}$ we have

$$\alpha = \Upsilon\{\gamma \in \mathbb{D}; \gamma \preccurlyeq \alpha\}; \quad (5)$$

- increasingly dense if the set $\{\gamma \in \mathbb{D}; \gamma \preccurlyeq \alpha\}$ is increasing to $\alpha$ for any $\alpha \in \mathbb{M}$.

Proposition 7: Let $\mathbb{A} \subset \mathbb{B}$ be specifically decreasing. Then we have $\bigwedge_{\odot}\mathbb{A} = \bigwedge\mathbb{A}$.

Proof: Let $\alpha^{'} = \wedge\mathbb{A}$. Then $\alpha^{'} \geq \bigwedge_{\odot}\mathbb{A}$. Let $\beta \in \mathbb{A}$ be fixed. It follows
$\alpha^{'} = \bigwedge\{\alpha \in \mathbb{A}, \alpha \leq_{\odot} \beta\}$. The family $\{\beta : \alpha; \alpha \in \mathbb{A}, \alpha \leq_{\odot} \beta\}$ is increasing and $\beta = \alpha \odot (\beta : \alpha)$ implies
$\beta = (\bigwedge\limits_{\alpha\in\mathbb{A},\ \alpha\leq_{\odot}\beta} \alpha) \odot (\bigvee\limits_{\alpha\in\mathbb{A},\ \alpha\leq_{\odot}\beta} (\beta : \alpha))$
for any $\alpha \in \mathbb{A}$, $\alpha \leq_{\odot} \beta$. It resulta that $\alpha^{'} \leq_{\odot} \beta$ and, therefore $\alpha^{'} \leq_{\odot} \bigwedge_{\odot}\mathbb{A}$.□

Proposition 8: Let $\mathbb{A} \subset \mathbb{B}$ be specifically increasing and dominated. Then we have $\bigvee_{\odot}\mathbb{A} = \bigvee\mathbb{A}$.

Proof: Let $\alpha^{'} = \bigvee\mathbb{A}$. Then $\alpha^{'} \leq \bigvee_{\odot}\mathbb{A}$. Consider an arbitrary $\beta \in \mathbb{A}$. We have
$\alpha^{'} = \bigvee\{\alpha \in \mathbb{A} \ / \ \alpha \geq_{\odot} \beta\}$. The family $\{\beta : \alpha;\ \alpha \in \mathbb{A}, \alpha \leq_{\odot} \beta\}$ is increasing and $\alpha = \beta \odot (\alpha : \beta)$ implies $\alpha^{'} = \beta \odot (\bigvee\limits_{\alpha\in\mathbb{A},\ \alpha\geq_{\odot}\beta} (\alpha : \beta))$ for any $\alpha \in \mathbb{A}$, $\alpha \geq_{\odot} \beta$.
We have $\alpha^{'} \geq_{\odot} \beta$ and $\alpha^{'} \geq_{\odot} \bigvee_{\odot}\mathbb{A}$.□

Corollary 9: The order topology $\tau_{\leq}$ is finer than the specific order topology $\tau_{\leq_{\odot}}$.

B2. Observability

Next we investigate the concept of observer, distinguishing between the discrete and continuous cases. The concept of discrete observer is now classical in the theory of event structures [2].

A discrete observer is a function $dob : \mathbb{B} \to \omega$ such that

$$\alpha \prec \beta \Rightarrow dob(\alpha) \prec dob(\beta).$$

An embedded process is called discrete observable if admits a discrete observer.
An embedded process is injectively observable iff there exists an injective discrete observer.

A continuous observer is a function $cob : \mathbb{B} \to \overline{\mathbb{R}}_{+}$ with the following properties:
($\mathrm{CO}_{\mathbf{1}}$) $\alpha \prec \beta \Rightarrow cob(\alpha) \leq cob(\beta)$, $(\forall \alpha, \beta \in \mathbb{B})$;
($\mathrm{CO}_{\mathbf{2}}$) $cob(\beta) = \sup_{i\in I}(cob(\beta_i))$ if $(\beta_i)_{i\in I} \uparrow \beta$;
($\mathrm{CO}_{\mathbf{3}}$) $(\forall \beta \in \mathbb{B})$ $(\exists (\beta_i)_{i\in I} \uparrow \beta)$: $cob(\beta_i) < \infty$.
A continuous observer $cob$ is called nondeterministic iff

$$cob(\alpha \odot \beta) = \max(cob(\alpha), cob(\beta)) \tag{6}$$

An embedded process is called continuous observable if admits a continuous observer.

The process image is

$$\begin{aligned} Im\mathbb{B} \quad = \quad & \{cob : \mathbb{B} \to \overline{\mathbb{R}}_{+}; \\ & cob \text{ is an additive continuous observer}\} \end{aligned} \tag{7}$$

Remark 2: $Im\mathbb{B}$ can be ordered with the usual pointwise order
$cob_1 \leq cob_2 \Leftrightarrow cob_1(\beta) \leq cob_2(\beta)$ $(\forall \beta \in \mathbb{B})$.
In this order $Im\mathbb{B}$ is a lattice and

$$(cob_1 \vee cob_2)_{(\beta)} = \sup_{\beta_1\odot\beta_2\leq\beta} \{cob_1(\beta_1) + cob_2(\beta_2)\}$$
$$(cob_1 \bigwedge cob_2)_{(\beta)} = \inf_{\beta_1\odot\beta_2=\beta} \{cob_1(\beta_1) + cob_2(\beta_2)\}$$

We state without proof the followings connections between observability and discreteness. The following properties can be easily adapted from similar results of [2].

If an embedded process is discrete observable then it is boundedly discrete. If the embedded process is countable then the converse also holds.
An embedded process is injectively observable iff the embedded process has finite intervals and it is countable.

B3. Algebraic properties of embedded processes

In the following, we show that an embedded process can be embedded into an ordered group. This allow us to prove further density results.

Let $\mathbb{A} \subset \mathbb{S}$ be a set such that $< \mathbb{A}, \leq_{\mathbb{A}} >$ satisfies the axioms $(P_3) \div (P_7)$. Define $[\mathbb{A}]$ as follows.
1. We introduce on $\mathbb{A} \times \mathbb{A}$ the following equivalence relation

$$(a, b) \approx (a^{'}, b^{'}) \Leftrightarrow a \odot b^{'} = a^{'} \odot b.$$

2. We denote by $[\mathbb{A}]$ the quotient space of $\mathbb{A} \times \mathbb{A}$. For any $a, b \in \mathbb{A}$ we denote by $\widehat{(a, b)}$ the element of $[\mathbb{A}]$ generated by $(a, b)$.

On $[\mathbb{A}]$ the following relations and operations can be defined:
- $\perp^{'} =: \widehat{(a, a)}$;
- $\widehat{(a, b)} \odot^{'} \widehat{(a^{'}, b^{'})} =: \widehat{(a \odot a^{'}, b \odot b^{'})}$;
- $\widehat{(a, b)} :^{'} \widehat{(a^{'}, b^{'})} =: \widehat{(a, b)} \odot^{'} \widehat{(b^{'}, a^{'})}$;
- $\widehat{(a, b)} \leq^{'} \widehat{(a^{'}, b^{'})}$ if $a \odot b^{'} \leq a^{'} \odot b$;
- $(\widehat{(a, b)})^{*} =: \widehat{(b, a)}$;
- $\widehat{(a, b)} \prec^{'} \widehat{(a^{'}, t^{'})}$ iff $\widehat{(a, b)}^{*} \prec \widehat{((a^{'}, b^{'}))^{*}}$.

Proposition 10: The map $a \to \widehat{a} = \widehat{(a, 0)}$ is a one-to-one and ordered-preserving map of $\mathbb{A}$ into $[\mathbb{A}]_{\uparrow} =: \{\widehat{a} \in [\mathbb{A}]; \widehat{a} \geq \perp\}$.

We define below the regular form of a function $a$, specified by a Hil term. This defines the weak solution of a differential equation that has the value of $a$ at the border. This concept gives an alternative semantics of the Hil $\wp.a$ operator.

For any $a \in [\mathbb{S}]$ we shall call the regular form of $a$ the element $\overline{a} \in \mathbb{B}$ defined by

$$\overline{a} = \bigwedge\{\beta \in \mathbb{B}; a \leq^{'} (\beta, \perp)\} \tag{8}$$

We can prove the following algebraic properties of the regular form.

Lemma 11: For any $a, b \in \mathbb{S}$
i) $\overline{a} \leq \overline{b}$ if $a \leq b$; ii) $\overline{a \odot b} \leq \overline{a} \odot \overline{b}$; iii) $\overline{(\overline{a})} = \overline{a}$;
iv) $(\overline{s_i})_{i\in I} \uparrow (\overline{s})$ if $(s_i)_{i\in I} \uparrow s$;
v) $(\overline{s_i})_{i\in I} \downarrow (\overline{s})$ if $(s_i)_{i\in I} \downarrow s$.

Proof:
i) Let $\mathbb{A} = \{\beta \in \mathbb{B} \ / \ a \leq^{'} (\beta, \perp)\}$ and $\mathbb{D} = \{\beta \in \mathbb{B} \ / \ b \leq^{'} (\beta, \perp)\}$. Then
$a \leq b \Rightarrow \mathbb{A} \supset \mathbb{D} \Leftrightarrow \bigwedge\mathbb{A} \leq \bigwedge\mathbb{D} \Leftrightarrow \overline{a} \leq \overline{b}$.
ii) Let $\mathbb{A} \odot \mathbb{D} = \{\beta \in \mathbb{B} \ / \ a \odot b \leq^{'} (\beta, \perp)\}$. Then
$\wedge(\mathbb{A} \odot \mathbb{D}) \leq (\wedge\mathbb{A}) \odot (\wedge\mathbb{D}) \Leftrightarrow \overline{a \odot b} \leq \overline{a} \odot \overline{b}$.
iii)-v) Results by direct calculations.□

The next lemma is the key to obtain more density results.

Lemma 12: Let $\alpha, \beta, \gamma \in \mathbb{B}$ with

$$\beta = \alpha \odot \gamma.$$

Then

$$\overline{\alpha} \leq {}_{\odot}\beta \text{ and}$$
$$\beta : \overline{\alpha} = \bigvee\{\sigma \in; \sigma \leq \gamma, \sigma \leq_{\odot} \beta\}.$$

Proof: Of course $\beta \leq \gamma \odot \overline{\alpha}$. According to the decomposition property
$(\exists \delta, \delta^{'} \in \mathbb{B})$: $\beta = \delta \odot \delta^{'}$ and $\delta \leq \gamma$, $\delta^{'} \leq \overline{\alpha}$.
From $\delta^{'} = \beta : \delta \geq \beta : \gamma$ it follows $\delta^{'} \geq \alpha$ and therefore $\delta^{'} \geq \overline{\alpha}$, hence $\delta^{'} = \overline{\alpha}$. If $\sigma \in \mathbb{B}$ is such that $\sigma \leq \gamma$ and $\sigma \leq_{\odot} \beta$ it follows $\beta : \sigma \in \mathbb{B}$, $\beta : \sigma \geq \alpha$ and therefore $\beta : \sigma \geq \overline{\alpha}$. From $\overline{\alpha} \odot \delta = \beta$ we deduce $\delta \geq \sigma$.□

Proposition 13: For any $\alpha, \beta \in \mathbb{B}$ we have

$$(\alpha \vee \beta) \leq_{\odot} (\alpha \odot \beta).$$

Proof: We have $\alpha \vee \beta = \overline{\alpha \vee_{[\mathbb{B}]} \beta} = \overline{(\alpha \odot \beta) : (\alpha \wedge \beta)}$ hence $(\alpha \vee \beta) \leq_{\odot} (\alpha \odot \beta)$.□

Lemma 14: Let $\mathbb{A} \subset \mathbb{B}$ and let $\beta \in \mathbb{B}$ be such that $\alpha \leq_{\odot} \beta$ $(\forall \alpha \in \mathbb{A})$. Then

$$\bigvee \mathbb{A} \leq_{\odot} \beta.$$

Proof: We first assume that $\mathbb{A}$ is increasing. It follows $\beta = (\bigvee \mathbb{A}) \odot (\bigwedge (\beta : \alpha))$ so $\bigvee\limits_{\alpha \in \mathbb{A}} \mathbb{A} \leq_{\odot} \beta$. We shall prove that $\mathbb{A}$ may be assumed increasing. Let $(\alpha_i)_{1 \leq i \leq n}$ be a finite subset of $\mathbb{A}$ and let $(\gamma_i)_{1 \leq i \leq n} \subset \mathbb{B}$ such that $\beta = \alpha_i \odot \gamma_i$, $(\forall i : 1 \leq i \leq n)$. It follows that $\bigvee\limits_{1 \leq i \leq n} \alpha_i = \overline{\beta : (\bigwedge \gamma_i)} \leq_{\odot} \beta$.□

Theorem 15: The space of basic occurrences $([\mathbb{B}], \leq^{'})$ is a conditionally complete lattice in the essential order.

Proof: Let $\mathbb{A} \subset [\mathbb{B}]$ specifically dominated and let

$$\mathbb{D} =: \{\beta \in [\mathbb{B}];\ \alpha \leq_{\odot} \beta,\ \forall \alpha \in \mathbb{A}\}.$$

It is no loss of generality to assume $\perp \in A$. Then we have $\mathbb{D} \subset \mathbb{B}$. Let now $\beta^{'} = \wedge \mathbb{D}$. Since for any $\alpha \in A$ and $\beta \in \mathbb{D}$: $\beta : \alpha \in \mathbb{B}$ we get $\beta^{'} : \alpha = \bigwedge\{\beta : \alpha;\ \beta \in \mathbb{D}\}$, $\beta^{'} : \alpha \in \mathbb{B}$ and therefore $\beta^{'} \in \mathbb{D}$. Let now $\beta \in \mathbb{D}$ be fixed and denote $\gamma = \beta : \beta^{'}$. Then from Prop. 12 $\exists d \in \mathbb{S} : d = \beta : \gamma$ and $d \leq \beta^{'}$. From
$\gamma = (\beta : \alpha) : (\beta^{'} : \alpha)$ $(\forall \alpha \in \mathbb{A})$
it follows $\gamma \leq_{\odot} \beta : \alpha$. Hence there exists $e \in \mathbb{B}$ such that
$\beta = \gamma \odot \alpha \odot e$, $d \odot \gamma = \gamma \odot \alpha \odot e$, $d = \alpha \odot e$.
This implies $\gamma \geq_{\odot} \alpha$ and $\gamma \geq \beta^{'}$. Thus $\gamma = \beta^{'}$, $\beta \geq \beta^{'}$ and therefore $\beta^{'} = \bigvee_{\odot} \mathbb{A}$.□

Lemma 16: Let $s \in [\mathbb{S}]$, $s = a : b$. Then

$$\overline{s} \leq_{\odot} a.$$

Proof: We have $a = s \odot b \leq \widehat{s} \odot b$. Let $a = a_1 \odot a_2$ with $a_1 \leq \overline{s}$ and $a_2 \leq b$. It follows $a = a_1 \odot a_2 \leq a_1 \odot b$ so $a_1 \geq a : b \geq s$. From definition of $\overline{s}$ results $a_1 \geq \overline{s}$. Then $\overline{s} = a_1 \leq_{\odot} a$.□

Theorem 17: The space of basic occurrences $\mathbb{B}$ is a lower complete lattice in the specific order.

Proof: Let $\mathbb{B}^{\odot}_{\alpha,\beta} =: \{\gamma \in \mathbb{B}; \gamma \leq_{\odot} \alpha, \gamma \leq_{\odot} \beta\}$

$$\mathbb{B}^{\odot}_{\alpha,\beta} =: \{\gamma \in \mathbb{B}; \gamma \leq_{\odot} \alpha, \gamma \leq_{\odot} \beta\}$$

and $\alpha, \beta \in \mathbb{B}$, $\gamma \in \mathbb{B}^{\odot}_{\alpha,\beta}$. It follows that there exists $\gamma_1, \gamma_2 \in \mathbb{B}$ such that

$$\gamma = \alpha \odot \gamma_1 = \beta \odot \gamma_2.$$

Let $\delta = \bigwedge\{\gamma; \gamma \in \mathbb{B}^{\odot}_{\alpha,\beta}\}$,
$\delta_1 = \bigwedge\{\gamma_1; \gamma \in \mathbb{B}^{\odot}_{\alpha,\beta}\}$, $\delta_2 = \bigwedge\{\gamma_2; \gamma \in \mathbb{B}^{\odot}_{\alpha,\beta}\}$.
From $\delta = \alpha \odot \delta_1 = \beta \odot \delta_2$ it follows $\delta \in \mathbb{B}^{\odot}_{\alpha,\beta}$. Let $\theta = \overline{\gamma : \delta}$. Then $\theta = \overline{\gamma_1 : \delta_1} = \overline{\gamma_2 : \delta_2}$. From the decomposition property there exists $\sigma, \sigma_1, \sigma_2 \in \mathbb{B}$ with $\sigma \leq \delta$ such that
$\gamma = \sigma \odot \theta$, $\gamma_1 = \sigma_1 \odot \theta$, $\gamma_2 = \sigma_2 \odot \theta$.
It follows that $\sigma \in \mathbb{B}^{\odot}_{\alpha,\beta}$, $\sigma = \delta$, $\delta \leq_{\odot} \gamma$.
Because $\gamma \in \mathbb{B}^{\odot}_{\alpha,\beta}$ is arbitrary, it follows $\delta = \alpha \bigwedge_{\odot} \beta$.□

Proposition 18: If $\mathbb{A} \subset \mathbb{B}$ is an substructure which is dense in order from below and specifically solid then $\mathbb{A}$ is increasingly dense.

Proof: Let $a, \beta \in \mathbb{A}$. From Prop. 13. results $a \vee \beta \in \mathbb{A}$. Thus $\mathbb{A}$ satisfies the axioms of a basic space which is increasingly dense in $\mathbb{S}$.□

Proposition 19: If the subsets $\mathbb{A}, \mathbb{A}^{'} \subset \mathbb{B}$ are solid and increasingly dense then $\mathbb{A} \cap \mathbb{A}^{'}$ is solid and increasingly dense.

Proof: Let $\alpha \in \mathbb{B}$ and denote $Y = \{x \in \mathbb{A} \cap \mathbb{A}^{'} / x \leq \alpha\}$ and for $y \in \mathbb{A}$ with $y \leq \alpha$ denote $Y_y = \{x^{'} \in \mathbb{A}^{'} / x^{'} \leq y\}$. Then $Y_y \subset Y$ and $\alpha \geq \bigvee Y \geq \bigvee\limits_{y \in X,\ y \leq a} \bigvee Y_y = \alpha$. For any $y_1, y_2 \in Y$ there exists $x \in X$ such that $y_1 \leq x \leq a$ and $y_2 \leq x$. Since $\mathbb{A}^{'}$ is increasingly dense there exists $x^{'} \in X^{'}$ with $y_1 \leq x^{'} \leq x$ and $y_2 \leq x^{'}$. Obviously $x^{'} \in \mathbb{A}$ and therefore $x^{'} \in Y$.□

## VI. Conclusions

In this paper, we have presented an integrated specification framework for embedded systems and other classes of systems functioning in real physical environments (reactive systems, hybrid systems, etc). We have developed two specification languages: a Hilbertian logic for the physical environment and a probabilistic process algebra for the concurrent transition system modelling the embedded controller. The integration mechanism is based on partially ordered sets and the gluing semantics relies on abstract algebra. We have investigated extensively this gluing semantics, creating in this way a semantic foundation for further developments.

The departing point of the Hilbertian logic is the fact that the designer of an intelligent controller should consider seriously the complex behaviours of physical environments. The methods of embedded system engineering have become very effective by oversimplifying the continuous dynamics. The different nature characterizing mathematical models of physical processes makes almost impossible the applications of formal methods to this area. It is not only the complexity of (partial) differential equations and stochastic process models that makes this area almost unapproachable, but often also the computational infeasibility: in many cases there is no explicit

representation of solutions available. Numerical approximations are very time consuming and logically inexpressive. The Hilbertian logic is an attempt of specifying solutions of such models inspired by the mathematical practice. The so-called weak solutions (or, more strictly speaking solutions in the sense of distribution theory) are introduced for the deterministic models. The key idea is to consider the largest class of functions having the known properties of the solutions (for example, functions that are Lebesgue squared integrable, right continuous, etc). The solutions are then characterised in this class of elements by axiomatic means or by advanced functional analysis methods like norm, Hilbert product, energy form, etc. The origin of this method are traced back to the monumental work of David Hilbert. We have shown [8], [9] that formal methods can be soundly founded on Hilbertian mathematics and thus calling them Hilbertian formal methods. An important body of this paper was devoted to develop this interpretation.

In a related paper [8], we have introduced a logic, called behavioural stochastic logic (BSL), for specifying the weak solutions of stochastic differential equations and Markov processes. The main difference between these logics (HiL and BSL) is that the semantics of BSL formulae are statements about probabilities of reachable sets. In fact, the two logics describe the duality between the deterministic - stochastic properties of the same physical phenomena. This suggests a connection in the form a unifying logic for continuous processes. In fact, our mathematical investigations related to the purpose of this paper show that Hil is more general than BSL. This statement can be mathematically formulated, but this constitutes the subject of a forthcoming paper. Actually, this is the idea behind to the choice of semi-dynamical systems. These and the Markov processes can be commonly axiomatized using semigroups of operators. To any semigroup one can associate a kernel operator, and, in this way, a Hilbertian logic. The semigroup of operators associated with a semi-dynamical system is presented in [15]. Some more elaborated mathematical arguments can show how the Hil logic associated to the semigroup of operators of a Markov process could be refined into a BSL logic.

The logic for the discrete controller must incorporate probabilistic features because the models of the HiL specifications it uses might be stochastic. Of course, a more realistic logic would have been stochastic, i.e. combining probability with real time. This issue constitutes a nice direction for feature work.

The future work will focus on applying this model to the synthesis of embedded process controllers. For the deterministic case, there is already an impressive body of research in applying formal methods to continuous dynamical systems pioneered and extensively developed by Pappas, Tabuada and coworkers (see [14] and the references therein).

## References


[1] Abramsky, S., Buneman, P., Gardner, P., Gordon, A., Kwiatkowska, M., Milner, R., Sassone, V., Stepney, S.: Science for Global Ubiquitous Computing A fifteen-year Grand Challenge for computing research. UK National e-Science Centre publication. Available from www.nesc.ac.uk/esi/events/Grand_Challenges/proposals/Ubiq.pdf

[2] E. Best, C. Fernandez "Non-Sequential Processes" EATCS Monograph in Theoretical Computer Science, Springer-Verlag, 1990.

[3] N. Boboc, G. Bucur, A. Cornea "Order and Convexity in Potential Theory. H-Cones" Lecture Notes in Math, vol 853, Springer Verlag, Berlin, 1981.

[4] M.L. Bujorianu, M.C.Bujorianu: A Model Checking Strategy for a Class of Performance Properties of Fluid Stochastic Models. In M. Telek e.a. eds., Proceedings of 3rd European Performance Engineering Workshop, Springer LNCS 4054, 2006.

[5] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: Bisimulation for General Stochastic Hybrid Systems. In M. Morari and L. Thiele (Eds.), Proc. Hybrid Systems: Computation and Control, 8th International Workshop, LNCS 3414, pp. 198-216, 2005.

[6] M.C. Bujorianu, M.L. Bujorianu: Constructive Stochastic Analysis: Foundations and Applications Research Report 2/2002 Computing Laboratory, University of Kent, 2002.

[7] Bujorianu, M.L., Bujorianu, M.C.: Distributed Stochastic Hybrid Systems. In Horacek P., Simandl M., Zitek P. (Eds.), "Proceedings of the 16th IFAC World Congres" 2005.

[8] Bujorianu, M.L., Bujorianu, M.C.: Behavioural Stochastic specification submitted.

[9] Bujorianu, M.L., Bujorianu, M.C.: Formal Specification of Stochastic Embedded Systems submitted.

[10] M.L. Bujorianu, J. Lygeros. General Stochastic Hybrid Systems: Modelling and Optimal Control. 43th IEEE Conference in Decision and Control, 2004.

[11] European Commission HYBRIDGE project: Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time System Design www.nlr.nl/public/hosted-sites/hybridge/

[12] C. J. Fidge, I. J. Hayes, and B. P. Mahony. Defining differentiation and integration in Z. Second IEEE International Conference on Formal Engineering Methods (ICFEM'98), IEEE Computer Society Press, pp. 64-73, 1998.

[13] M. Fukushima: "Dirichlet Forms and Markov Processes" North Holland, 1980.

[14] Haghverdi, E., Tabuada, P., Pappas, G.J.: Bisimulation Relations for Dynamical, Control and Hybrid Systems. Theoretical Computer Science, Vol. 342, no. 2-3, pp. 229-261, 2005.

[15] Hmissi, M.: Semi-groupes Deterministes. Sem. Th. Potentiel 9 (1989), Paris, in Lect. Notes in Math, (1393) 135-144.

[16] J-P. Katoen, R. Langerak, D. Latella Modelling systems by probabilistic process algebra: an event structures approach. Formal Description Techniques (FORTE'93), pp. 253-268, North-Holland, 1994.

[17] J-P. Katoen: Qualitative and Quantitative Extensions of Event Structures. Ph.D thesis, University of Twente, 1996.

[18] D. Noble, Y. Rudy: "Models of cardiac ventricular action potentials: Iterativeinteraction between experiment and simulation". Philosophical Transactions: Mathematical, Physical and Engineering Sciences, 359, pp. 1127-1142, 2001.

[19] C.A. Petri: Concurrency as a Basis of Systems Thinking. Proc. from 5th Scandinavian Logic Symposium, 1979.

[20] G. Pola, M.L. Bujorianu, J. Lygeros, M. D. Di Benedetto. Stochastic Hybrid Models: An Overview with Applications to Air Traffic Management. ADHS, Analysis and Design of Hybrid System, Saint-Malo, 2003.

[21] P. Saperstone, Semidynamical Systems in Infinite Dimensional Spaces. Appl. Math. Sci. 37, Springer, Berlin 1981.

[22] J. Woodcock, J. Davies Using Z Prentice Hall, 1996.